Une « monnaie numérique de banque centrale », c'est quoi ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 juin 2021

https://www.bortzmeyer.org/monnaie-numerique-banque.html

Dès qu'il s'agit de monnaie, on lit n'importe quoi dans les médias, et on entend n'importe quoi aux tribunes des colloques. Songeons par exemple à tous les gens qui ont péroré sur le Bitcoin ou sur les cryptomonnaies sans rien y connaitre. De même quand on parle de « monnaie numérique de banque centrale », la confusion règne. Notons donc un excellent article d'analyse écrit pour la banque centrale suisse (mais qui n'exprime pas la politique officielle de cette institution) expliquant à quoi pourrait ressembler une MNBC (monnaie numérique de banque centrale) et proposant une solution spécifique.

Lorsqu'on parle de « monnaie électronique » (ou numérique), la confusion règne. Parfois, le terme désigne toute monnaie qui n'est pas en pièces ou en billets (à ce compte, toutes les monnaies sont électroniques depuis longtemps). Parfois, on ne le dit que pour les cryptomonnaies ou que pour celles qui tournent sur une chaine de blocs. Ici, on va utiliser le terme pour une monnaie qui a certaines propriétés de l'argent liquide (notamment une certaine protection de la vie privée) tout en étant entièrement numérique. Ainsi, la carte Visa n'entre pas dans cette définition, car elle n'offre aucune vie privée.

L'article dont je parlais au début est « Comment émettre une monnaie numérique de banque centrale <https://www.snb.ch/fr/mmr/reference/working_paper_2021_03-fr/source/working_paper_2021_03-fr.fr.pdf> ». Oui, l'avantage des études faites pour un organisme officiel suisse, c'est qu'il y a une traduction de qualité en français. Ses auteurs sont David Chaum (celui de DigiCash), Christian Grothoff (celui de GNUnet) et Thomas Moser, des gens qui connaissent leur sujet, donc.

Pour résumer leur article (mais je vous en recommande la lecture complète), leur cahier des charges est celui d'une monnaie émise et gérée par une banque centrale (un cahier des charges, donc, très différent de celui du Bitcoin, qui vise à se passer de banque centrale), garantissant un minimum d'anonymat pour ceux qui paient avec cette monnaie (« la préservation d[Caractère Unicode non montré [1]]une propriété clé de la monnaie physique : la confidentialité des transactions »), mais pas pour ceux qui

1. Car trop difficile à faire afficher par LaTeX

la reçoivent. Les revenus des commerçants ne sont donc pas dissimulés, ce qui permet de lutter contre la fraude fiscale. La définition même de monnaie ne fait pas consensus mais les auteurs se focalisent sur un rôle, le moyen d'échange (il y en a d'autres rôles à la monnaie, par exemple unité de mesure ou stockage de valeur). De plus, les auteurs veulent appliquer les principes de KYC (connaissance du client), d'AML (lutte contre le blanchiment) et de CFT (lutte contre le financement du terrorisme), oui, il y en a, des sigles, dans le secteur bancaire. On voit que les objectifs mis en avant sont distincts de ceux de Bitcoin et, a fortiori, de Zcash puisque que, comme le note l'article, « La détection de fraude requiert cependant une capacité d[Caractère Unicode non montré]identification du payeur et le traçage des clients, ce qui est incompatible avec le respect de la confidentialité de la transaction. ». Le fait d'avoir un cahier des charges clair est un des intérêts de cette étude. Par exemple, d'innombrables articles ont été écrits sur des projets comme Diem ou le « yuan électronique » alors que leur cahier des charges reste vague. Le problème est d'autant plus grave qu'il y a souvent de la mauvaise foi dans certains discours. Ainsi, les projets de numérisation ont souvent pour but réel d'en finir avec l'argent liquide pour avoir une traçabilité complète des transactions et une surveillance permanente des acheteurs.

Comment les auteurs de l'article voient-ils leur système de MNBC (monnaie numérique de banque centrale) ? Étant donné qu'il n'y a qu'un émetteur, nul besoin d'une chaine de blocs. (La quasi-totalité des projets de « chaine de blocs privée » ou de « chaine de blocs à permission » n'ont aucun sens : comme le dit l'article « La DLT est une architecture intéressante lorsqu[Caractère Unicode non montré]il n[Caractère Unicode non montré]existe pas d[Caractère Unicode non montré]acteur central ou si les parties prenantes ne souhaitent pas s[Caractère Unicode non montré]accorder sur un acteur central de confiance. Ce qui n[Caractère Unicode non montré]est cependant pratiquement jamais le cas pour une monnaie numérique de détail émise par une banque centrale. [...] Recourir à un registre distribué [réparti, plutôt] ne fait qu[Caractère Unicode non montré]augmenter les coûts de transaction ; cela n[Caractère Unicode non montré]apporte aucun avantage dans une mise en place par une banque centrale »). Leur système repose à la place sur GNU Taler (développé par un des auteurs) et les signatures en aveugle de Chaum. La sécurité du système dépend donc de ces techniques logicielles. (D'autres propositions font appel à des systèmes physiques spécifiques, mais « les fonctions physiques non clonables ne peuvent pas s[Caractère Unicode non montré]échanger sur Internet (éliminant de fait l[Caractère Unicode non montré]usage principal de la MNBC » et « les tentatives précédentes de verrous matériels pour empêcher la copie ont été compromises de façon répétée », voir les DRM.) Comme la monnaie numérique de banque centrale envisagée dans cet article a beaucoup de propriétés communes avec l'argent physique (le liquide), elle a également une sécurité proche : possession fait loi, ce qui veut dire que, si l'appareil sur lequel vous gardez vos pièces est détruit, vous perdez votre argent. Cette solution, comme l'argent liquide, n'est raisonnable que pour des sommes relativement faibles. Si l'acheteur n'est pas identifiable, le vendeur l'est car il ne peut pas réutiliser directement les « pièces », il doit les remettre à la banque. C'est nécessaire au mécanisme de protection contre la double dépense. Autre nécessité, la banque centrale doit être connectée en permanence, ce qui impose des exigences nouvelles pour les banques centrales (« La détection de doubles dépenses en ligne élimine ce risque mais rend donc les transactions impossibles si la connexion Internet de la banque centrale est indisponible. ») Je ne vous détaille pas les protocoles cryptographiques ici, je n'ai pas le niveau, lisez l'article. Notez qu'ils sont assez complexes, ce qui peut être un obstacle à l'adoption : la plupart des utilisateurs ne peuvent pas comprendre cette solution, ils devront faire confiance à la minorité qui a compris et vérifié. (Ceci dit, dès aujourd'hui, peu de gens comprennent le système monétaire.)

Quelles sont les chances qu'une banque centrale, avec ses messieurs sérieux en costume-cravate, reprenne cette idée et se lance dans un projet de monnaie numérique protégeant la vie privée ? Personnellement, je dirais qu'elles sont à peu près nulles. Les auteurs notent à juste titre que « une MNBC de détail devrait être basée sur un logiciel libre ou ouvert. Imposer une solution propriétaire qui entraînerait une dépendance à un fournisseur spécifique pourrait vraisemblablement constituer dès le départ un obstacle à son adoption. » Mais cette condition suffirait à faire rejeter le projet par toute banque centrale (déjà, le mot « libre »…). Tous ces dirigeants politiques et financiers passent du temps à critiquer le Bitcoin « qui permet la fraude fiscale et le financement du terrorisme » mais ils ne font aucun effort pour développer des alternatives. Le projet décrit dans cet article est sympathique mais n'a aucune chance. Il essaie de

plaire aux banques centrales mais celles-ci n'en voudront jamais, attachées qu'elles sont à des solutions fermées, privatrices, et facilitant la surveillance.

---

https://www.bortzmeyer.org/monnaie-numerique-banque.html